

**ORIGINAL**

AO 91 (Rev. 11/82)

**CRIMINAL COMPLAINT**

UNITED STATES DISTRICT COURT		CENTRAL DISTRICT OF CALIFORNIA	
UNITED STATES OF AMERICA v. MICHAEL ALAN GOLDBERG DONNICA RABULAN JAMES CALEB KUEKER		DOCKET NO.	
		MAGISTRATE'S CASE NO. <b>19 MJ00784</b>	
Complaint for violation of Title 21, United States Code, Section 846			
NAME OF MAGISTRATE JUDGE <b>THE HONORABLE ALKA SAGAR</b>		UNITED STATES MAGISTRATE JUDGE	LOCATION Los Angeles, California
DATE OF OFFENSE May 21, 2018	PLACE OF OFFENSE Los Angeles County	ADDRESS OF ACCUSED (IF KNOWN)	<div style="border: 1px solid black; padding: 5px;">                         FILED  <b>CLERK, U.S. DISTRICT COURT</b>  <div style="border: 1px solid black; padding: 2px; display: inline-block;">                             MAR - 1 2019                         </div> </div> CENTRAL DISTRICT OF CALIFORNIA BY <span style="float: right;">AS</span> DEPUTY
COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION: <p style="text-align: center;">[21 U.S.C. § 846]</p> <p>Beginning on a date unknown, but no later than May 21, 2018, and continuing to present, defendants MICHAEL ALAN GOLDBERG, DONNICA RABULAN, and JAMES CALEB KUEKER, together with others known and unknown, conspired and agreed with each other to knowingly and intentionally distribute over 500 grams of a mixture and substance containing a detectable amount of methamphetamine, in violation of Title 21, United States Code, Sections 841(a)(1), (b)(1)(A)(viii).</p>			
BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED: <p style="text-align: center;">(See attached affidavit which is incorporated as part of this Complaint)</p>			
MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A			
Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.	SIGNATURE OF COMPLAINANT <b>ANDREW KIM</b>		
	OFFICIAL TITLE Special Agent – Homeland Security Investigations		
Sworn to before me and subscribed in my presence,			
SIGNATURE OF MAGISTRATE JUDGE <sup>(1)</sup> 		<b>ALKA SAGAR</b>	DATE March 1, 2019

<sup>(1)</sup> See Federal Rules of Criminal Procedure 3 and 54

**AFFIDAVIT**

I, Andrew Kim, being duly sworn, declare and state as follows:

**I. PURPOSE OF AFFIDAVIT**

1. This affidavit is made in support of a criminal complaint and arrest warrant against Donnica Rabulan ("RABULAN"), Michael Alan Goldberg ("GOLDBERG"), and James Caleb KUEKER ("KUEKER"), for a violation 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances).

2. This affidavit is also made in support of an application for a warrant to search 8419 Wakefield Avenue, Panorama City, CA 91402 ("SUBJECT PREMISES 1"), as described more fully in Attachment A-1, 12029 Tiara Street, Valley Village, CA 91607 ("SUBJECT PREMISES 2"), as described more fully in Attachment A-2, 2275 Vasanta Way, Los Angeles, CA 90068 ("SUBJECT PREMISES 3"), as described more fully in Attachment A-3, the person of RABULAN, as described more fully in Attachment A-4, and the person of KUEKER, as described more fully in Attachment A-5, for fruits, evidence, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 21 U.S.C. § 953 (exportation of controlled substances), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 1956 (laundering of monetary instruments), 18 U.S.C. § 1957 (engaging in monetary transactions in property from specified unlawful activity), and 18 U.S.C. § 371 (conspiracy) (the "SUBJECT OFFENSES").

3. This affidavit is also submitted in support of an application for a combined criminal and civil forfeiture seizure warrant for the following assets, including all funds -- currency, cryptocurrency, private keys, and recovery seeds -- that may be located during execution of the requested search warrants, as well as all such items stored in, or accessible via, wallets for digital currency controlled by RABULAN, GOLDBERG, and KUEKER in the Central District of California.

## **II. SOURCES OF INFORMATION**

4. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and have been so employed since September 2015. I am currently assigned to the HSI Office of the Assistant Special Agent in Charge in El Segundo, California as part of the International Mail Facility Border Enforcement Security Taskforce ("IMF BEST"), which is responsible for investigating trafficking violations involving international mail. Before working with HSI, I was a Border Patrol Agent with the United States Border Patrol, an agency within DHS, for approximately eight years.

5. In 2007, I attended and completed the United States Border Patrol Academy in Artesia, New Mexico. In 2015, I attended and completed the Criminal Investigator Training Program and HSI SA Training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. Through my training, I learned of HSI's criminal investigative authority, as well as investigative techniques for performing criminal

investigations. HSI is responsible for enforcing federal criminal statutes prohibiting, among other things, the distribution of and possession with intent to distribute drugs, in violation of Title 21 of the United States Code. During my employment with DHS, I have investigated drug smuggling through the United States Mail and other mail courier services in and out of the United States. I have executed search warrants to seize evidence of violations of federal and state law, as well as arrest warrants to apprehend individuals who have committed such violations.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

7. I have discussed this case in detail with HSI SA Christopher Hicks. SA Hicks is assigned to HSI's Northridge office, and previously the Cyber Financial Group, which is responsible for investigating financial crimes involving the use of computers and technology. He has been employed by HSI since April 2015. His duties include the investigation of violations of federal criminal law, particularly those laws found in Titles

8, 18, 19, and 21 of the United States Code, and relating to financial fraud, computer fraud, immigration, customs, and drugs. As a result of his training and experience, SA Hicks is familiar with federal laws concerning access device fraud, wire fraud, mail fraud, money laundering, customs, drug, and immigration violations, as well as cryptocurrency, the darknet, and the TOR network (described in Section V).

8. I have also discussed this case in detail with USSS SA David Schwartz. SA Schwartz is assigned to the Los Angeles Electronic Crimes Task Force, which is responsible for investigating cybercrimes, including crimes related the criminal activity on the Dark Net, cyber enabled fraud, and network intrusions. SA Schwartz has been employed by the USSS since April 2016. SA Schwartz has investigated cases involving the operation of unlicensed cryptocurrency exchanges, illicit Dark Net activity, as well as fraud. SA Schwartz has also received training in drug investigations and participated in investigations related to the trafficking of controlled substances.

### **III. SUMMARY OF PROBABLE CAUSE**

9. On May 24, 2018, Customs and Border Protection ("CBP") officers notified HSI agents that seven DHL parcels shipped from the United States to the Philippines contained a combined total of approximately 20.85 kilograms of methamphetamine. Employees at the UPS Store where four of the seven seized parcels were mailed identified RABULAN as one of two people who shipped the four parcels containing methamphetamine. The UPS Store

employees also identified GOLDBERG and RABULAN, who are married, as people who previously shipped international parcels from that store.

10. CBP also seized six additional international United States Postal Service ("USPS") parcels containing methamphetamine. Surveillance footage shows RABULAN mailing two of the seized parcels on May 29, 2018. One parcel contained approximately 72 grams of methamphetamine and was destined for Australia; the second parcel contained approximately one kilogram of methamphetamine and was destined for New Zealand.

11. Video footage from a post office in Van Nuys, CA shows GOLDBERG mailing a parcel to Poland on or about May 30, 2018 (the "POLAND PARCEL"). Cell phone records show that a number subscribed to GOLDBERG tracked the POLAND PARCEL through the USPS website on June 5, 2018, and that an IP address at SUBJECT PREMISES 1 also tracked the POLAND PARCEL on June 2, 2018. Polish authorities discovered approximately 2 kilograms of methamphetamine inside the POLAND PARCEL.

12. While detained at the Metropolitan Detention Center ("MDC") since June 6, 2018, GOLDBERG has made numerous phone calls to RABULAN, often using other inmates' phone lines, to discuss drug trafficking, destruction of evidence, and the movement of currency. RABULAN and GOLDBERG's marriage certificate states that SUBJECT PREMISES 1 is their residence. Surveillance and utility records confirm that RABULAN continues to reside at SUBJECT PREMISES 1.

13. GOLDBERG's recorded jail calls with KUEKER also show that KUEKER assisted GOLDBERG and RABULAN with the drug trafficking operation by collecting and safekeeping drug proceeds at KUEKER's residence, moving and destroying evidence, and by hiding GOLDBERG and RABULAN's assets from the federal government. KUEKER's assistance has allowed GOLDBERG to continue to traffic drugs while in prison. KUEKER has also used a counterfeit driver's license to write a \$30,000 fraudulent check to GOLDBERG. KUEKER resides at SUBJECT PREMISES 2 and 3, as determined by surveillance, cell-site records, recorded jail calls, and other documents, as discussed in further detail below.

#### **IV. STATEMENT OF PROBABLE CAUSE**

14. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

##### **A. Background on CBP International Package Inspection**

15. Based on my training and experience and my conversations with fellow law enforcement officers, I know the following:

a. CBP must first examine and admit international mail parcels and shipments that arrive in the United States before they are delivered to their destinations by a carrier, including the USPS. CBP officers are assigned to International Mail Facilities ("IMFs") like the facility in Torrance, California. CBP officers conduct routine examinations of foreign mail service parcels at the IMF in Torrance, California

as the parcels enter the United States before the parcels are prepared for delivery to their final destination. Due to the large volume of cargo that enters the United States on a daily basis, CBP is unable to examine all parcels. CBP uses a variety of methods to select parcels for border search examination, including random and targeted inspections.

b. International Express Mail parcels shipped from the United States to other countries using privately owned mail carriers, such as DHL, are subject to examination by its employees. When these companies discover contraband, the companies notify CBP and CBP seizes the package.

c. Pursuant to their authority under Title 19, Code of Federal Regulations, Section 162.6 (also known as "Border Search Authority"), CBP officers and certain other law enforcement officers may conduct examinations of goods entering the United States without a search warrant, probable cause, or individualized suspicion.<sup>1</sup>

**B. RABULAN Shipped Methamphetamine to the Philippines in May 2018**

16. On May 22 and 23, 2018, a DHL Security Manager in Van Nuys, California contacted CBP Officers regarding seven parcels destined for the Philippines that DHL suspected of containing controlled substances. CBP Officers examined the parcels and

---

<sup>1</sup> From my conversations with the United States Attorney's Office, I am also aware of the following case law holding that searches at the border do not require probable cause or a warrant: United States v. Ramsey, 431 U.S. 606, 619 (1977); see also United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc).



discovered methamphetamine with a combined weight of 20.85 kilograms.

17. The details of the seven seizures and consignor information, as determined by my review of DHL records, the contents of the packages, and laboratory reports, follows:

a. Parcel #1

DHL Tracking Number: 2568796624  
Commodity: Wire Shelving Rack  
Contraband: 4.7 kilograms of methamphetamine

Consignor:

Tracy Shapoff  
3727 Magnolia Blvd., Burbank, CA 91505.  
Phone number: 818-747-3247

b. Parcel #2

DHL Tracking Number: 2568778380  
Commodity: Comforter Set  
Contraband: 2.01 kilograms of methamphetamine

Consignor:

Tracy Shapoff  
3727 Magnolia Blvd., Burbank, CA 91505.  
Phone number: 818-747-3247

c. Parcel #3

DHL Tracking Number: 3544444886  
Commodity: Comforter Set  
Contraband: 2 kilograms of methamphetamine

Consignor:

MGA Production  
18618 Clark St., Tarzana, CA 91356.  
Phone number: 818-747-3247

d. Parcel #4

DHL Tracking Number: 3544446850  
Commodity: Comforter Set  
Contraband: 2.05 kilograms of methamphetamine

Consignor:

Danica Santiago  
19360 Rinaldi St., #710, Porter Ranch, CA 91326.  
Phone number: 818-919-8758

e. Parcel #5

DHL Tracking Number: 9792736483  
Commodity: Office Chair  
Contraband: 2.02 kilograms of methamphetamine

Consignor:

Donna Cruz  
9141 Le Mona Ave., Apt. 115, North Hills, CA  
91343.  
Phone number: 818-919-8758

f. Parcel #6

DHL Tracking Number: 9792752115  
Commodity: Shelf Rack  
Contraband: 4.05 kilograms of methamphetamine

Consignor:

Donna Cruz  
9141 Le Mona Ave., Apt. 115, North Hills, CA  
91343.  
Phone number: 818-919-8758

g. Parcel #7

DHL Tracking Number: 6853172970  
Commodity: Shelf Rack, Chocolate Candy  
Contraband: 4.02 kilograms of methamphetamine

Consignor:

Kenneth Kwuan  
15215 Los Alimos St., Mission Hills, CA 91345.  
Phone number: 747-206-0784

18. Six of the parcels listed the consignor phone number 818-919-8758 or 818-747-3247. According to T-Mobile records that I reviewed, Alan Goldberg Contractors at 19360 Rinaldi St.,

Apt 710, Porter Ranch CA 91326,<sup>2</sup> was the subscriber for phone number 818-919-8758 from January 26, 2018, to April 25, 2018, and for the phone number 818-747-3247 from July 31, 2017, to February 13, 2018. T-Mobile records also show that GOLDBERG registered both phone numbers in his name. The seventh parcel was shipped to a similar consignee as parcel number four ("Raymond Herreras" and "Ramon Hernandez"), contained approximately the same amount of methamphetamine as parcel number six (4000 and 4050 grams), had the same description as parcel number six ("Shelf Rack"), and was shipped to the same destination country as parcels one through six (Philippines) and the same destination city as parcels one, two, three, and six (Quezon).

19. Four of the parcels' consignor addresses have ties to either GOLDBERG or RABULAN: According to law enforcement databases, GOLDBERG previously resided at 18618 Clark St., Tarzana, CA 91356 which was used for parcel #3. Law enforcement databases also show that RABULAN previously resided at 9146 Le Mona Ave., Apt. 115, North Hills, CA 91343, which is similar to the address used for parcels #5 and #6, 9141 Le Mona Ave., Apt. 115, North Hills, CA 91343.

20. Parcels 1 through 4 were mailed from UPS Store #2398 located at 19360 Rinaldi Street, Porter Ranch, CA 91326 (the "UPS Store").

---

<sup>2</sup> As described in ¶ 21, this address is from a UPS Store box that GOLDBERG rented. Based on review of GOLDBERG's jail calls and Alan Goldberg's social media profile, I believe that GOLDBERG's father is "Alan Goldberg."

21. On May 30, 2018, I interviewed employees at the UPS Store. Based on California Driver License ("CDL") photographs of GOLDBERG and RABULAN, employees identified GOLDBERG as a longtime customer and the renter of Box 710 at the UPS Store and RABULAN as the person they knew as "Danica Santiago," the listed shipper of parcel #4. According to a UPS Store employee, on May 21, 2018, RABULAN and her friend entered the UPS Store together and mailed parcels 1 through 4. RABULAN mailed parcel #3 under the consignor name MGA Productions and parcel #4 under the consignor name Danica Santiago. RABULAN's friend, mailed parcels 1 and 2 under the consignor name "Tracy Shapoff."

**C. RABULAN Shipped Methamphetamine Parcels to the Philippines and GOLDBERG Shipped a Methamphetamine Parcel to Poland**

22. On June 5, 2018, the Philippine media reported the arrest of four individuals in the Philippines following a controlled delivery of methamphetamine by the Philippine Drug Enforcement Agency ("PDEA"). The news report stated that the drugs were shipped from a "Dona Santiago" from addresses including 2700 Cahuenga Boulevard, Los Angeles, California, and 3737 Burnet, North Hills, California.

23. As a result, CBP began investigating USPS parcels shipped from 2700 Cahuenga Boulevard and 3737 Burnet. Based on my review of records, conversations with officers from CBP and other law enforcement agencies, and my own investigation in this case, I understand the following:

24. On June 6, 2018, CBP officers at the IMF inspected a USPS parcel, bearing the tracking number EZ010907245US (the "NEW

ZEALAND PARCEL"), that consignor "Jeff Stevens" at 2700 E. Cahuenga Boulevard, Los Angeles, CA 90068 shipped to an address in New Zealand, and discovered 1.04 kilograms of methamphetamine. Based on my review of law enforcement databases, there is no "Jeff Stevens" at that address or the Tarzana address below, and thus I believe that the shipper of these parcels used a false name to hide their identity from law enforcement.

25. On June 11, 2018 CBP officers at the IMF targeted and inspected another USPS parcel, bearing the tracking number EZ010910686US, from consignor "Jeff Stevens" at 2700 E. Cahuenga Boulevard, Los Angeles, CA 90068 shipped to Australia and discovered approximately 72.6 grams of methamphetamine (the "AUSTRALIA PARCEL").

26. "Jeff Stevens" also shipped three other parcels internationally around the same time as the NEW ZEALAND PARCEL and the AUSTRALIA PARCEL. CBP seized two of the parcels, which contained a total of 176.1 grams of methamphetamine. The consignor address for these shipments was 3160 Pastel Avenue, Studio City, CA 91604, which is similar to GOLDBERG's father's address at 3760 Pastel Place, Studio City, CA 91604.

27. On June 7, 2018, CBP Officer Lionel Andrade notified me of the POLAND PARCEL that was in transit to consignee Patryk Breczko in Piensk, Poland. The consignor of the POLAND PARCEL was "Jeff Stevens" at 18618 Clark Street, Tarzana, California. Due to previous seizures attributed to consignor "Jeff Stevens" and a consignor address at 18618 Clark Street, I notified HSI

agents in Frankfurt, Germany, who in turn notified the Polish authorities that the POLAND PARCEL might contain methamphetamine.

28. On June 9, 2018, the Centralne Biuro Sledcze Policji ("CBSP") Warsaw advised HSI agents that they seized a package containing approximately 2 kilograms of methamphetamine and arrested two subjects who attempted to pick up the POLAND PARCEL at the postal office in Poland.

29. Post-seizure analysis identified that in May 2018, a USPS parcel, bearing the tracking number EZ010908427 ("POLAND PARCEL 2"), weighing 4.33 kilograms was successfully mailed to consignee Milosz Balcerzak in Piensk, Poland. The consignor of this parcel was Chuck Tontana at 3737 Burnet, North Hills, CA 91343. The contents of POLAND PARCEL 2 were not tested. However, on July 22, 2018, CBSP Warsaw advised HSI agents that they arrested two additional subjects for their involvement in the smuggling of methamphetamine, including Milosz Balcerzak, the recipient of POLAND PARCEL 2.

30. I have identified a total of 59 international mail parcels that I believe are part of GOLDBERG and RABULAN's scheme to distribute drugs based on a combination of the consignor name, consignor address, consignee name, and consignee address. Shippers mailed these parcels to the Philippines, Australia, New Zealand, the United Kingdom, Italy, Poland, and France. Fourteen of the 59 parcels have been seized in the United States containing a total of approximately 22.3 kilograms of methamphetamine and 170 grams of marijuana. Authorities in

other countries have seized four of the 59 parcels containing approximately 2.1 kilograms of methamphetamine.

31. I reviewed video surveillance of individuals mailing the POLAND PARCEL, the NEW ZEALAND PARCEL, and the AUSTRALIA PARCEL. Based on my review of the video, I believe RABULAN mailed at least four parcels, including the AUSTRALIA PARCEL and the NEW ZEALAND PARCEL, from a post office in Northridge, CA on May 29, 2018. Based on my review of video from a post office in Van Nuys, California and a comparison with GOLDBERG's CDL photograph, I believe GOLDBERG mailed the POLAND PARCEL from that post office on May 30, 2018.

32. Based on USPS records and records from Charter Communications, I know that a user from an IP address assigned to SUBJECT PREMISES 1 tracked the POLAND PARCEL on June 5, 2018, on the USPS website. As discussed below, RABULAN lives at SUBJECT PREMISES 1 and GOLDBERG did as well until his detention at MDC on June 6, 2018. This IP address is also registered to SUBJECT PREMISES 1, but to a name I believe is fictitious because it does not appear in any law enforcement database. The phone number on the account for this second IP address at SUBJECT PREMISES 1 is registered to GOLDBERG. In addition, T-Mobile records show that a user with a phone number registered to GOLDBERG tracked the POLAND PARCEL on the USPS website from a second IP address on June 5, 2018.

**D. GOLDBERG's Debit Card Paid for Methamphetamine Shipments**

33. Based on my review of GOLDBERG's bank records, I understand he currently has an account at Radius Bank in his name and with the same address as Box 710 at the UPS Store. HSI SA Hicks received confirmation that Radius Bank issued a debit card ending in 1882 to GOLDBERG.

34. Based on my review of GOLDBERG's Radius Bank records, I know that on May 2, 2018, his debit card ending in 1882 paid the postal fees for the USPS parcels with tracking numbers EZ120042002US and EZ120041996US at a post office in Studio City, CA. CBP intercepted the USPS parcel with tracking number EZ120042002US, and that parcel contained approximately 45 grams of methamphetamine. CBP did not intercept the USPS parcel with tracking number EZ120041996US, and it was delivered to New Zealand.

35. Based on my review of GOLDBERG's Radius Bank records, I also know that on May 7, 2018, his debit card ending in 1882 paid the postal fees for a USPS parcel with tracking number EZ010910712US at a post office in Panorama City, CA. The Australian Border Force intercepted the USPS parcel with tracking number EZ010910712US, and it contained approximately 28 grams of methamphetamine. The debit card ending in 1882 also paid to ship the USPS parcel with tracking number EZ010908427, described above as POLAND PARCEL 2, weighing 4.33 kilograms. As described above, CBP did not intercept POLAND PARCEL 2, but based on the consignor name, consignor address, and item



description for POLAND PARCEL 2 that matched another seized shipment containing methamphetamine, and the arrest by Polish authorities of the intended recipient of POLAND PARCEL 2 for methamphetamine distribution, I suspect that POLAND PARCEL 2 also contained methamphetamine.

**E. RABULAN and GOLDBERG's Residence is SUBJECT PREMISES 1**

36. Based on my review of a certified copy of GOLDBERG and RABULAN's marriage certificate, I learned that GOLDBERG and RABULAN applied for a marriage license on May 29, 2018, and were officially married the following day. The address listed on their marriage certificate is SUBJECT PREMISES 1.

37. On September 17, 2018, SA Hicks conducted surveillance at SUBJECT PREMISES 1 and saw a silver BMW bearing California license plate 7CDG300. A vehicle registration check of the BMW revealed that its owners are RABULAN and Manolita Rabulan.

38. On October 4, 2018, SA Hicks conducted surveillance at SUBJECT PREMISES 1 and saw a red Maserati with dealer license plates. In a jail phone call between GOLDBERG and RABULAN, RABULAN stated that she wanted to purchase a used Maserati for approximately \$60,000.

39. On October 17, 2018, USSS SA David Schwartz conducted surveillance at SUBJECT PREMISES 1 and saw a Land Rover Range Rover parked on the sidewalk near SUBJECT PREMISES 1's driveway. The Range Rover, bearing California license plate N613M0, is registered to RABULAN at SUBJECT PREMISES 1.

40. Based on my review of public utility records on November 28, 2018, and Special Agent Loan McIntosh's

conversation with a Los Angeles Department of Water and Power ("LADWP") employee on February 25, 2019, RABULAN has held an LADWP account in her name at SUBJECT PREMISES 1 since May 23, 2018, through at least the date of my review (February 25, 2019).

41. SA Christopher Hicks informed me that on or about December 31, 2018, he saw RABULAN on the same street as SUBJECT PREMISES 1 driving a Maserati, a vehicle that previous surveillance saw parked by the sidewalk in front of SUBJECT PREMISES 1 on or about December 26, 2018.

42. On January 16, 2019, while conducting surveillance, SA Hicks saw a female inside the garage at SUBJECT PREMISES 1 who appeared to be RABULAN based on a comparison with her CDL photograph.

43. On February 27, 2019, SA Hicks and SA Schwartz saw both the Range Rover registered to RABULAN and the Maserati in the driveway of SUBJECT PREMISES 1. On that date, SA Hicks and SA Schwartz also saw an individual they believe to be RABULAN (based on her CDL photograph) in the driveway of SUBJECT PREMISES 1.

**F. GOLDBERG and RABULAN Discuss Drug Trafficking in MDC Phone Calls**

44. On June 6, 2018, GOLDBERG surrendered to law enforcement for an outstanding warrant for mail theft and fraud. As of January 2019, GOLDBERG is in custody at the MDC in Los Angeles, CA. Based on my review of jail calls and conversations with other agents, I understand that at MDC inmates are allotted

300 minutes every month to make outgoing phone calls. GOLDBERG has used approximately sixteen other inmates' phone accounts to talk beyond his monthly 300 minutes, and he is also using their accounts in an attempt to conceal his conversations about the sale of drugs and the destruction of evidence from law enforcement. When GOLDBERG uses his own phone account, he repeatedly states that he cannot freely discuss things.

45. I have listened to over a hundred MDC phone calls made by GOLDBERG, and I am able to recognize and identify GOLDBERG, RABULAN, and KUEKER's voices based on their speech patterns, quality/tone of their voices, and how they identify themselves during calls. A person who wants to receive phone calls from an inmate at MDC must register their phone number and receive approval with the Federal Bureau of Prisons ("BOP"). Based on names provided to BOP, five phone numbers belonging to RABULAN and one phone number belonging to KUEKER have been registered with BOP. The BOP tracks and categorizes jail calls made to phone numbers belonging to RABULAN and KUEKER's which has assisted me in identifying who GOLDBERG is calling. Below are a sample of calls in which GOLDBERG and RABULAN discussed the conspiracy to distribute drugs:

46. On June 14, 2018, at approximately 6:42 a.m., GOLDBERG made an MDC phone call from his own account to RABULAN. GOLDBERG and RABULAN discuss the inability to talk freely because he is on his MDC phone account. GOLDBERG states, "Hey can you answer the other phone number today? The 310 number because I'm not going to call you on this number today. . . ."

Baby, answer the other phone, I can't be talking to you like this for reals."

47. Several hours later, at approximately 10:05 a.m., GOLDBERG made an MDC phone call using inmate Joseph Hill's phone account to RABULAN. The conversation begins with RABULAN, GOLDBERG, and an individual only known as "Echo" on a three-way phone call. GOLDBERG stated that RABULAN will "handle it today or tomorrow" which I believe, based on the context of the exchange, is referring to the shipment of drugs and money transfers. After Echo hangs up, GOLDBERG and RABULAN continue their conversation about money an individual named "Rain" owes them. GOLDBERG states, "Make sure you get 25% before you do anything. . . . The rest of them make sure, especially Rain. I want 25 grand of the money he owes me." Based on the context of the conversation and my investigation of the case, I believe the "25 grand" to refer to the proceeds from drug sales.

a. GOLDBERG and RABULAN then discuss checking GOLDBERG's P.O. boxes because they "should all be hitting" and that "it's" sitting there. Based on my investigation of this case, I believe "it's" refers to incoming drug shipments GOLDBERG will then sell via a Dark Net marketplace or proceeds from drug trafficking.

b. GOLDBERG and RABULAN begin to discuss how much to pay people to cover shipping costs. RABULAN asks, "How much do I pay for the shipping?" GOLDBERG replies, "It depends how heavy, if they're big \$1600, but if they're light \$500 each one." Records from the UPS Store #2398 -- where four DHL

parcels containing methamphetamine were shipped from -- show that RABULAN paid \$405.92, \$455.29, \$640.38, and \$455.29 for the shipping fees, which is consistent with GOLDBERG's statements that a "light" parcel costs \$500 to ship.

c. GOLDBERG and RABULAN continue their conversation by discussing the logistics for selling drugs and use the term "loss." Based on my training, experience, and investigation of this case, I understand that the use of the term "loss" in this context refers to the value of drugs seized prior to delivery to its intended target. GOLDBERG inquires, "Who are you sending it to? Echo and who else? Call Rain. . . . I only really care about Rain because that's a big thing right there. And they all owe me money so they got to pay." RABULAN replies, "They want you to cover the loss." GOLDBERG responds, "I'm willing to cover more than half. The original deal was half the losses. I'm willing to cover 75% of the loss. . . . Look, tell them to shoot at least 25% of the loss." The conversation continues with the discussion of drug sales using "DM," or the Dark Net Marketplace Dream Market, to Poland and Australia.

48. At approximately 5:49 p.m., GOLDBERG made another MDC phone call from inmate Joseph Hill's phone account to RABULAN. RABULAN states, "I was just speaking to Kai on the phone. He said his balance is only 12,000." GOLDBERG responds, "12, then he has to pay 3,000 dollars. Did he lose all his shipments?" RABULAN states, "Yea he did." GOLDBERG replies, "Then he has to pay only 3,000." I understand this exchange to be consistent

with GOLDBERG's earlier statement that he will cover 75% of all losses on drug shipments.

49. On June 6, 2018, at approximately 9:20 a.m., GOLDBERG made an MDC phone call to RABULAN and RABULAN's older sister, Donna Mae Rabulan. In the conversation, the parties discuss getting access to the dark web, destroying evidence, and the status of drug shipments. GOLDBERG instructs RABULAN, "Tell your sister to clean out the shredder." RABULAN relays the message to her sister and asks, "I don't know the login for the other thing . . . the darkweb." GOLDBERG begins to respond, "It's 'Drugs R Us'" but is promptly interrupted by RABULAN and Donna Mae Rabulan from saying anything further over the phone.

a. Later in the conversation, RABULAN says, "Babe. I was online yesterday. It was all bad. Oh my gosh, oh my gosh. That's all I'm going to say." GOLDBERG asks, "How many did they get? A lot? All of them?" RABULAN replies, "I've seen everything that you've dinged. Like everything. Everything." GOLDBERG responds, "So, they got every last thing that we've sent? That's crazy. Look, let me tell you something right now, if it doesn't pop off, return that one thing to the Mexicans, the Paisas." Based on my investigation of this case, I believe GOLDBERG and RABULAN were referring to the fourteen parcels seized by CBP in the United States and other parcels seized by the PDEA in the Philippines containing methamphetamine in late May and early June 2018. I also believe that the Mexicans or Paisas are GOLDBERG's drug supplier.

50. On June 18, 2018, at approximately 2:00 p.m., GOLDBERG made an MDC phone call to KUEKER instructing him and RABULAN to destroy evidence. GOLDBERG states, "One time, cop, I don't know if it was an undercover or a marked car followed someone leaving yesterday. . . . Yeah and where they were leaving to is 'OT.'<sup>3</sup> . . . But like have her get everything out dog, everything, you know. They are going to hit my pad. Like I'm positive that they are going to hit that motherfucker. You know what I mean, and I can't have nothing happen to her. Do whatever you got to do and figure it out." Based on my training and experience and investigation of this case, I understand that GOLDBERG is instructing KUEKER to assist RABULAN in removing or destroying evidence located in GOLDBERG and RABULAN's home in advance of a search by law enforcement.

51. On June 26, 2018, in an MDC conversation between GOLDBERG and RABULAN, RABULAN states that "Ben" wanted more drugs from RABULAN. RABULAN says, "He's like [quoting Ben] 'I've got people begging me for that, I mean I can move it quick. . . . Can you ask him to front you a small amount at first like a quarter of it . . . ?'" GOLDBERG interjects, "Baby, just kill all that, I don't want to talk about that. That's too much talking. . . . Tell him unless he has all the money. It's no. End of story, tell him Mike said no. I don't want to front money to people no more." Based on my training and experience,

---

<sup>3</sup> Based on my training and experience, in this context "OT" refers to "off the record" and is used to describe a location associated with illicit activity and is used to avoid recognition by law enforcement.

in this call, RABULAN is discussing the potential sale of drugs on credit to an individual identified as Ben. I believe "Ben" refers to Benjamin Meir ("MEIR"), an individual who resides with KUEKER at SUBJECT PREMISES 3. MEIR provided the BOP his email address so that he could be added as a contact for GOLDBERG.

52. On October 17, 2018, in an MDC phone call, GOLDBERG asks KUEKER, "Where's Ben at?" KUEKER replies, "He's right here. Do you want to say hi?" An individual I believe to be MEIR comes on the phone and says, "What up dog?" GOLDBERG tells MEIR that he had to take him off as an MDC email contact because, "I got in trouble dog, you're fucking dumb dog. Why would you write some shit about fucking freezer bags dude? Come on dog, they're all monitored. . . . Shut up dog, I'm trying not to catch another indictment." Based on this call, I believe GOLDBERG and MEIR have distributed drugs together prior to GOLDBERG's arrest on June 6, 2018. Further, the call reflects that GOLDBERG believed MEIR has knowledge of GOLDBERG's criminal activity that could result in additional criminal charges for GOLDBERG if MEIR were to reveal this information on a monitored email.

53. On October 15, 2018, in an MDC phone call between GOLDBERG and KUEKER, KUEKER states that he is doing the "books" with "V". It is my belief that "books" refers to the ledger that KUEKER is safekeeping for GOLDBERG that details the profits from drug proceeds, commonly known as "pay-owe" sheet. I believe "V" is Valerie Ramirez ("RAMIREZ") who has also funded MDC inmates' phone accounts for GOLDBERG to use. CBP databases



show that Valerie Ramirez receives international shipments at SUBJECT PREMISES 2, and I believe Ramirez also resides at SUBJECT PREMISES 3 based on surveillance conducted by SA Schwartz.

**G. KUEKER Funds GOLDBERG's MDC Phone Calls and Discusses Drug Trafficking with GOLDBERG**

54. Based on my review of MDC phone records, from June 7, 2018, to October 8, 2018, at the request of GOLDBERG, KUEKER deposited a total of \$1,325 into thirteen other inmates' MDC phone accounts. As discussed above, GOLDBERG used other inmates' phone accounts in an attempt to evade detection by law enforcement when discussing the distribution of drugs and the destruction of evidence. Because calls made from MDC include a warning that calls are recorded, I believe that GOLDBERG is aware that law enforcement can monitor calls made from his phone account. As a result, GOLDBERG is careful to not openly discuss incriminating topics when making phone calls from his own phone account. GOLDBERG also uses shorthand or coded language when discussing his criminal activities. Unless otherwise specified, the contents of the conversations included in this affidavit are as translated based on my training and experience and knowledge of this investigation.

55. On June 7, 2018, in an MDC phone call, GOLDBERG asks KUEKER, "And everything came in too?" KUEKER replies, "Yeah, yeah, yes it did. And I just need to know basically what to do ... how to." GOLDBERG says, "You take it all with you. . . . They are \$5 each one, \$5 apiece. . . . The other thing is minimum

\$10,000." KUEKER responds, "Gotcha. Ok, yeah, gotcha."

GOLDBERG then instructs KUEKER, "Hold my money until I get out, yeah? How much money did you pick up from my girl last night, like 15? . . . In an envelope?" KUEKER states, "Yeah, yeah, there were two envelopes." Based on my investigation of this case, I believe that in this call GOLDBERG and KUEKER discussed the distribution of drugs and that KUEKER acts as a custodian for GOLDBERG's drugs and money while GOLDBERG is in prison.

56. On June 20, 2018, in an MDC phone call between KUEKER and GOLDBERG, they discussed ordering and selling drugs. GOLDBERG says, "You guys should really look into reordering, dawg." KUEKER replies, "Yeah, Yeah. I just want to make sure that there's not too much in stock, you know." GOLDBERG also tells KUEKER that his life story would be more interesting than the drug traffickers in "Cocaine Cowboy," a documentary that features several Miami cocaine traffickers during the 1970's and 1980's. GOLDBERG states, "I was reading this book about this Cocaine Cowboy and I was like this fool is fucking weak. . . . I really want to do a movie and book when I get out. I think I'll make enough money for everybody to get out of the game." KUEKER responds, "I saw this from the very beginning. Man, damn this would be a great fucking documentary." GOLDBERG says, "And this will be in the book too, about you calling me in the feds."

57. On July 13, 2018, in an MDC phone call between KUEKER and GOLDBERG, they discussed the arrest of one of their associates who federal agents arrested for dropping off or picking up a package from the post office. GOLDBERG cautioned

KUEKER to drop his phone number because his contact information would be in the arrestee's phone contact list. KUEKER stated that he planned to activate two new phone lines soon.

58. On July 23, 2018, in an MDC phone call between KUEKER and GOLDBERG, GOLDBERG asks what happened to their "thing in 'DM.'" I understand that DM is the abbreviation for the Dark Net marketplace named "Dream Market" which is often used to buy and sell drugs. KUEKER states that RABULAN placed another order and that he plans to go to the post office and check for its arrival. GOLDBERG suggests that KUEKER should order from DM himself using Bitcoins and contact the DM vendor, Don Cimura, and split profits with him.

59. On September 5, 2018, in an MDC phone call, KUEKER informs GOLDBERG that he would get together with RABULAN to "straighten that one thing" and to let her know what he was doing. GOLDBERG replies, "Did you go through Don, the one I told you. Don Cimura?" KUEKER replies, "Yeah." In this conversation, I believe KUEKER confirms that he purchased drugs from Don Cimura via "DM" using Bitcoins. On October 2, 2018, in an MDC phone call, GOLDBERG tells KUEKER that RABULAN was waiting for "more things to come in" and that KUEKER should contact "Don" using Wickr. GOLDBERG instructs KUEKER to download Wickr<sup>4</sup> because "it's the safest way" and that's "how he talks to him."

---

<sup>4</sup> Wickr is an encrypted mobile communication application that automatically deletes text messages after a set time.

**H. KUEKER Protects GOLDBERG's Drug Proceeds**

60. Based on my review of MDC phone calls, GOLDBERG instructed KUEKER to move items from his residence at SUBJECT PREMISES 1 to KUEKER's residence because GOLDBERG believed that federal agents were going to search SUBJECT PREMISES 1.

61. MDC phone calls also show that GOLDBERG wanted his vehicles to be stored at KUEKER's residence because Federal Probation Officers planned to conduct asset checks on GOLDBERG. GOLDBERG also suggested that the Maserati that RABULAN had recently purchased be placed under KUEKER's name, and KUEKER agreed. KUEKER suggested finding a car storage unit to hide all of GOLDBERG's vehicles.

62. MDC phone calls between GOLDBERG and RABULAN show that KUEKER keeps track of GOLDBERG's proceeds from drug trafficking in a notebook or ledger. Based on a review of jail calls and my investigation of this case, I believe that this ledger is being kept inside a safety deposit box in SUBJECT PREMISES 2 or 3. GOLDBERG stated that KUEKER is keeping approximately \$80,000 in U.S. currency and 10 to 14 Bitcoins for him. GOLDBERG referred to the cash KUEKER was safekeeping as his "nest egg" for when he gets out of jail. The ledger may also be referring to a digital device known as a Nano Ledger where cryptocurrency can be stored offline. In a phone call on July 24, 2018, KUEKER tells GOLDBERG that the cryptocurrency that RABULAN gave him was sent to his Nano Ledger, a device that keeps a detailed record of cryptocurrency transactions. GOLDBERG replies that he wants to send KUEKER more cryptocurrency.

63. CBP Import records show that KUEKER received international mail parcels at SUBJECT PREMISES 2 that were described as containing Nano Ledgers in March and July 2018.

64. On July 9, 2018, in an MDC phone call, KUEKER informed GOLDBERG that they were "very well off [from] one of those things to Germany." I believe KUEKER is referencing to a successful shipment of methamphetamine to Germany. GOLDBERG then instructs KUEKER to hold onto the profits for him.

**I. KUEKER Resides at SUBJECT PREMISES 2 and 3**

65. In a September 28, 2018, recorded jail call with GOLDBERG, KUEKER stated that he currently lives near the intersection of Oxnard Street and Laurel Canyon Boulevard. Based on my review of a map, SUBJECT PREMISES 2 is one block south of the intersection at Oxnard Street and Laurel Canyon Boulevard.

66. On an October 17, 2018, recorded call, KUEKER states that he plans to keep his old residence but also plans to rent a property in the Hollywood Hills area with five bedrooms as a "second place" with an individual named "Ben." Based on my review of public records, SUBJECT PREMISES 3 is in the Hollywood Hills and has six bedrooms.

67. On November 6, 2018, through California vehicle registration checks, SA Schwartz identified KUEKER's vehicle as a 2016 Lincoln bearing California license plate 7TFC411 registered to the same address as SUBJECT PREMISES 2 and registered to KUEKER.

68. On or about December 31, 2018, SA Hicks conducted surveillance and saw KUEKER's vehicle on the driveway of SUBJECT PREMISES 2. On or about January 24, 2019, SA Schwartz saw KUEKER's vehicle at SUBJECT PREMISES 3.

69. Based on my review of public utility records on November 28, 2018, and Special Agent Loan McIntosh's conversation with a LADWP employee on February 25, 2019, KUEKER has held an LADWP account in his name at SUBJECT PREMISES 2 since January 27, 2017, through at least February 25, 2019.

70. On January 15, 2019, United States Magistrate Judge Frederick F. Mumm issued a warrant authorizing the disclosure of GPS and cell-site information, commonly known as pings, for KUEKER's cellular phone. Based on my conversation with SA Schwartz, I understand that from January 15, 2019, to January 25, 2019, pings demonstrate that KUEKER's cellular phone was: (1) in the area of SUBJECT PREMISES 2 overnight for five out of ten nights; (2) in the area of SUBJECT PREMISES 3 overnight for the remaining five nights; and (3) in the area of SUBJECT PREMISES 2 and 3 during the daytime. I also understand that from February 18, 2019, to February 28, 2019, pings demonstrate that KUEKER's cellular phone was: (1) in the area of SUBJECT PREMISES 2 overnight for five out of ten nights; (2) in the area of SUBJECT PREMISES 3 overnight for the remaining five nights; and (3) in the area of SUBJECT PREMISES 2 and 3 during the daytime.

71. USPIS Postal Inspector Kyle Reyes confirmed that as of January 25, 2019, KUEKER still receives mail at SUBJECT PREMISES

2 in his name. In addition to KUEKER, six other people live at or frequent SUBJECT PREMISES 3 based on surveillance. As described above, at least two individuals in addition to KUEKER are involved in his drug operation to some extent.

**J. KUEKER Picks Up Parcels From GOLDBERG's P.O. Box**

72. On June 5, 2018, I interviewed two employees at the UPS Store, where GOLDBERG rents P.O. Box #710.<sup>5</sup> Based on these interviews, I understand that between May 30, 2018, and June 5, 2018, GOLDBERG gave the UPS Store employees instructions that KUEKER would pick up the mail on his behalf for Box #710. On January 1, 2019, SA Hicks, SA Schwartz, and PI Reyes spoke with employees at the UPS Store and learned that KUEKER and "Scott" were picking up mail at this location for Box #710. On November 3, 2018, in an MDC phone call between GOLDBERG and KUEKER, GOLDBERG instructed KUEKER to pick up mail from Box #710.

73. Based on my review of records and conversations with other agents, I understand that there are several international inbound seizures associated with Box #710. On January 20, 2018, CBP seized 16 grams of MDMA addressed to "Michael Gold" at Box #710. On February 10, 2018, CBP seized 50 tablets of MDMA addressed to "Michael Gold" at Box #710. On April 16, 2018, CBP seized 929 tablets of MDMA addressed to "Mike Gold" at Box #710.

---

<sup>5</sup> As noted above, this is the same location where RABULAN mailed four DHL parcels to the Philippines containing methamphetamine.

**K. KUEKER Deposits a Fraudulent Check in GOLDBERG's Account**

74. Based on a review of records from Fidelity Investments, checks in the amounts of \$65,034.18, \$30,000, and \$10,000 were deposited into GOLDBERG's account. Fidelity flagged these deposits as fraudulent and reversed the transactions.

75. For the \$30,000 deposit, a check (#004503) from "David Allen Cox" on behalf of Affordable Housing Partners was made out to GOLDBERG as partial payment for a loan. A copy of the check dated November 27, 2017, shows that a "David Allen Cox" signed it. Fidelity Investment notes associated with this \$30,000 deposit stated that the identity of "David Allen Cox" was verified by "DL," which I understand to mean driver's license. Fidelity Investments records for this transaction contained a copy of a Virginia driver's license bearing the name "David Allen Cox" with a date of birth of August 15, 1978. The image on the scanned copy of the Virginia driver's license bore the image of KUEKER based on a comparison with KUEKER's CDL. I thus believe that KUEKER attempted to deposit the fraudulent \$30,000 check in GOLDBERG's account using the Virginia driver's license in the name of "David Allen Cox."

**L. Use of Cryptocurrency to Facilitate Drug Trafficking**

76. Based on my training and experience and having conferred with agents familiar with cryptocurrency, I am familiar with online/Dark Net drug trafficking websites, including the Dark Net marketplace named "Dream Market" or "DM."



I understand that digital currency like Bitcoin is the method of payment for Dark Net drug transactions. I also know that drug traffickers move, hide, and obfuscate their digital currencies into different accounts. They also use unlicensed money remitters to avoid reporting requirements and government oversight.

77. Radius Bank records provided to SA Hicks show that GOLDBERG's Radius Bank account had funds transferred to it from GOLDBERG's Coinbase account. Coinbase is a U.S. based company that exchanges a digital currency like Bitcoin, Ethereum, and Litecoin for fiat currency or vice versa.

78. Based on my review of records and conversations with other agents, I understand that the source of GOLDBERG's digital currency on Coinbase may be the proceeds of illicit means.

79. A review of GOLDBERG's finances show funds totaling \$231,548.77 moved from Coinbase into GOLDBERG's Radius Bank account.

80. Deposit application data from the Radius Bank account listed GOLDBERG's mailing address as 19360 Rinaldi Street, #710 Porter Ranch, CA 91326, the same addresses used to ship multiple international parcels containing methamphetamine.

81. A query for GOLDBERG's, RABULAN's, and KUEKER's employment history through the California Employment Development Department shows no employment history. There is no indication that GOLDBERG, RABULAN, and KUEKER have any source of legitimate income.

82. As noted above, GOLDBERG instructed KUEKER to order from "Don" on "DM" using Bitcoins. Based on a subsequent jail call, I believe KUEKER confirmed that he ordered from "Don" on "DM" using Bitcoins. Other jail calls show that KUEKER is holding Bitcoins for GOLDBERG and that KUEKER received cryptocurrency. Based on my investigation of this case, I believe that GOLDBERG, KUEKER, and RABULAN's cryptocurrency is the proceeds or involved in the trafficking of drugs.

**M. Additional Suspicious Financial Transactions**

83. Based on my review of bank records, on June 9, 2018, RABULAN deposited \$25,000 into her Wells Fargo account from GOLDBERG's Radius Bank account.

84. On June 16, 2018, GOLDBERG emailed "Donnica Goldberg" at Dannrabulan@gmail.com through his MDC email instructing RABULAN to have KUEKER pretend to be GOLDBERG to call Radius Bank. GOLDBERG told RABULAN that she should know his last four digits of his social security number and provided RABULAN his mother's maiden name.

85. On July 30, 2018, SA Hicks received a telephone call from Radius Bank Investigator, David Oliveira, stating that an individual claiming to be GOLDBERG tried to withdraw \$40,000 from GOLDBERG's account, but Radius Bank had frozen the account due to suspicious transactions. The individual called from GOLDBERG's cellular phone and provided Radius Bank GOLDBERG's full name, birthday, last four of his Social Security number, and mother's maiden name to gain access to the account.

86. On October 16, 2018, SA Hicks received a response from Wells Fargo containing records of five accounts owned by RABULAN. A review of these accounts contained the following information.

	Accounts	Credits	Debits
a.	1949473894	3,807.36	3,857.36
b.	3948839117	23,245.82	24,924.24
c.	5355186312	208,998.08	206,210.64
d.	7204408483	12,108.22	12,108.22
e.	8238620804	24,420.08	23,020.08
f.	Grand Total	272,579.56	270,120.54

87. Many of the transactions show patterns of large amounts of money deposited and then quickly withdrawn. Based on my training and experience and investigation of this case, I believe that the large amounts of deposits and quick withdrawals demonstrate that GOLDBERG and RABULAN are funneling drug proceeds. The following are examples of transactions from RABULAN's Wells Fargo bank accounts:

- a. On March 30, 2018, \$3,000 was deposited and then the same amount was withdrawn on April 2, 2018.
- b. On April 5, 2018, \$40,000 was deposited. Later in the day \$27,000 was withdrawn. On the following day, \$12,000 was withdrawn.
- c. On April 13, 2018, \$2,000 was deposited and the same amount was withdrawn the same day.

88. Based on my review of RABULAN's bank records, I understand that she deposited \$40,000 into her Wells Fargo Bank account from Gregory Werber. Agents in another investigation have identified Werber as an unlicensed money remitter dealing with the exchange of cryptocurrency. In an MDC phone call, GOLDBERG instructed RABULAN to sell Werber their twelve Bitcoins.

89. On December 5, 2018, DEA, HSI, USSS, and USPIS executed an arrest warrant for Gregory Werber and search warrants for Werber's residence and business located in Manhattan Beach, California. Law enforcement arrested Werber for laundering the drug proceeds for a Mexican-based drug trafficking organization.

90. During the search of Werber's residence, I found a handwritten note in Werber's bedroom with the following information:

Michael Alan Goldberg  
76444-112  
2:17-CR-00786-CJC

Kraut Law Group  
Anthony Christopher Rios  
Michael Eric Kraut

(323) 464-6455  
464-6453

Judge Cormac J. Carney  
DOB: 1985

91. Based on my review of public records, I understand that the Kraut Law Group is the law firm representing GOLDBERG

for separate mail theft/fraud charges. Based on a jail call, I believe that GOLDBERG paid this law firm approximately \$135,000.

92. I believe the financial transactions detailed above, Werber's ties to Mexican drug traffickers, Werber's involvement with cryptocurrency, and Werber's \$40,000 deposit to RABULAN, provide further evidence that RABULAN, GOLDBERG, and KUEKER are involved in drug trafficking and money laundering using cryptocurrency.

#### V. BACKGROUND ON DIGITAL CURRENCY

93. Based on my training and experience, I am aware of the following concepts:

a. The "dark web," also sometimes called the "dark net" or "deep web," is a colloquial name for a number of extensive, sophisticated, and widely used criminal marketplaces operating on the Internet, which allow participants to buy and sell illegal items, such as drugs, firearms, and other hazardous materials with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply "web"). These online black market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. A famous dark web marketplace, Silk Road, operated similar to legitimate commercial websites such as Amazon and eBay, but offered illicit goods and services. Law enforcement shut down Silk Road in 2013. Cellular "smart phones" can connect to the internet, including the dark web, and can be used to manage a

drug vendor account as well as conduct digital currency transactions.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts." Customers, meanwhile, operate "customer accounts." It is possible for the same person to operate one or more customer accounts and one or more vendor accounts at the same time.

c. The "Tor network," or simply "Tor," is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a major dark-web browser known as "Tor Browser," designed to access the Tor network. One of the logos, or "icons," for Tor Browser is a simple image of the Earth with purple water and bright green landmasses with bright green concentric circles wrapping around the planet to look like an onion.

d. Digital currency (also known as cryptocurrency or virtual currency)<sup>6</sup> is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States and may be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

e. "Bitcoin" (or "BTC") is a type of online digital currency that allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. Bitcoins are a decentralized, peer-to-peer form of electronic currency having no association with banks or governments. Users store their bitcoins in digital "wallets," which are identified by unique electronic "addresses." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access Bitcoins on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an

---

<sup>6</sup> For purposes of this affidavit, "digital currency," "cryptocurrency," and "virtual currency" address the same concept.

account number while the private key is like the password to access that account. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the "Blockchain," the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

f. Although they are legal and have known legitimate uses, bitcoins are also known to be used by cybercriminals for money-laundering purposes, and are believed to be the most oft-used means of payment for illegal goods and services on "dark web" websites operating on the Tor network. By maintaining multiple bitcoin wallets, those who use bitcoins for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplace.

g. Bitcoin is one example of a digital currency; other digital currencies, such as Ethereum and Monero, also exist and are used by darknet actors. The technology underlying these currencies are similar, though these currencies provide more privacy and anonymity of the users.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a



PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code<sup>7</sup> with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

---

<sup>7</sup> A QR code is a matrix barcode that is a machine-readable optical label.

i. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

j. Darknet marketplaces often only accept payment through digital currencies, such as Bitcoin, and operate an escrow whereby customers provide the digital currency to the marketplace, who in turn provides it to the vendor after a

transaction is completed. Accordingly, large amounts of Bitcoin sales or purchases by an individual can be an indicator that the individual is involved in drug trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who have received Bitcoins as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoins to convert them to fiat (government-backed) currency. These individuals use exchange services offered on the darknet, whereby a darknet vendor who has received digital currency for sales can exchange that digital currency for fiat currency anonymously.

#### **VI. FORFEITURE**

94. Title 18, United States Code, Section 981 ("civil forfeiture") provides that "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 or 1957 of this title, or any property traceable to such property" is subject to forfeiture to the United States. 18 U.S.C. § 981(a)(1)(A).

95. Title 18, United States Code, Section 982 ("criminal forfeiture") provides that the court, "in imposing sentence on a person convicted of an offense in violation of section 1956 or 1957 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property." 18 U.S.C. § 982(a)(1).

96. Title 21, United States Code, Section 881 provides that "[t]he following shall be subject to forfeiture to the United States and no property right shall exist in them: . . . All moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical in violation of this subchapter, all proceeds traceable to such an exchange, and all moneys, negotiable instruments, and securities used or intended to be used to facilitate any violation of this subchapter." 21 U.S.C. § 881(a)(6).

97. Title 21, United States Code, Section 853 provides that "[a]ny person convicted of a violation of this subchapter or subchapter II of this chapter punishable by imprisonment for more than one year shall forfeit to the United States . . . any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation." 21 U.S.C. § 853(a)(1).

98. For the reasons set forth herein, I submit that there is probable cause to believe that the cash and cryptocurrency constitute property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 and 18 U.S.C. § 1957, or are traceable to such property, and are, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1) (civil forfeiture) and pursuant to 18 U.S.C. § 982(a)(1) (criminal forfeiture).

99. I moreover submit that there is probable cause to believe that cryptocurrency constitutes (1) money, negotiable

instruments, securities or other things of value furnished or intended to be furnished in exchange for a controlled substance in violation of the Controlled Substances Act; (2) proceeds traceable to such an exchange; or (3) money, negotiable instruments, or securities used and intended to be used to facilitate a violation of the Controlled Substances Act. The cryptocurrency is therefore subject to forfeiture to the United States pursuant to 21 U.S.C. § 881(a)(6) (civil forfeiture) and pursuant to 18 U.S.C. § 982(a)(1) (criminal forfeiture).

100. Finally, I submit there is probable cause to believe that cash and cryptocurrency constitute property constituting, or derived from, any proceeds obtained, directly or indirectly, as the result of drug trafficking, and are therefore subject to forfeiture to the United States pursuant to 21 U.S.C. § 853(a) (criminal forfeiture). As property subject to forfeiture, these items may be seized pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(f).

101. With respect to seizure, 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture." For the reasons described below, I submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure the availability of the cash for forfeiture.

102. As further set forth below, there is a substantial risk that RABULAN's/GOLDBERG's/KUEKER's cryptocurrency will dissipate or otherwise become unavailable for forfeiture unless immediate steps are taken, upon the execution of the requested searches, to secure RABULAN's/GOLDBERG's/KUEKER's cryptocurrency(ies).

103. Thus, I seek authority to (1) compel RABULAN, GOLDBERG, and KUEKER to put one or more of their fingers on their cell phone(s) to unlock the device(s); and (2) access their wallets (via applications on RABULAN's, GOLDBERG's, and/or KUEKER's cell phone(s)) for the purpose of transferring all of RABULAN's GOLDBERG's, and/or KUEKER's bitcoin or other cryptocurrency stored in or accessible via their wallets to a law enforcement-controlled bitcoin/cryptocurrency wallet. The seized cryptocurrency will then be preserved pending further forfeiture proceedings.

104. Per this affidavit and associated warrant applications, the government also seeks authorization to search RABULAN's, GOLDBERG's, and KUEKER's cell phones, digital devices such as iPads and computers, and cold storage devices, for, among other things, any additional bitcoin or cryptocurrency wallets for the purpose of seeking any additional follow-up wallets if appropriate.

**VII. TRAINING AND EXPERIENCE ON DRUG TRAFFICKING AND MONEY  
LAUNDERING**

105. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In

addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their drugs and may keep stashes of drugs in their vehicles in the event of an unexpected opportunity to sell drugs arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug



trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

i. The prices for one kilogram of methamphetamine in the following countries are approximately as follows:

- i. Australia / New Zealand = \$100,000 USD
- ii. Philippines = \$92,000 USD
- iii. Poland = \$ 51,000 USD

106. Drug dealing is a cash business. Customers pay for drugs with cash and dealers commonly purchase drugs from their suppliers with cash. Drug dealers commonly keep large sums of currency, financial instruments, precious metals, jewelry, and other items of value which represent either the proceeds from drug sales or are intended for the purchase controlled substances. When drug dealers amass such wealth, they often attempt to legitimize that wealth or otherwise conceal it and its origin from discovery by law enforcement. To accomplish this, drug dealers often use different techniques, including the use of foreign and domestic banks and their attendant services, including savings and checking accounts, securities, cashier's

checks, money drafts and letters of credit to exchange drug proceeds into money that appears to come from a legitimate source. Drug dealers also purchase real estate or vehicles and establish shell corporations and business fronts that they use to launder drug proceeds. Drug dealers often use fictitious or "straw-holder" owners to conceal the true ownership, vehicles, or other valuable items purchased with the proceeds of illicit drug sales. In addition, drug dealers often use wire transfers, cashier's checks, and money orders to pay for drugs or other costs relating to their distribution business. Drug dealers often keep these items of value, and records relating to them, on their person or in their residences, stash houses, and/or vehicles where they are concealed from law enforcement and readily available.

107. Drug dealers often use the United States Postal Service or commercial express mail delivery companies, such as FedEx or UPS, to ship drugs and money to various points within the United States. They do so, at least in part, due to the convenience of the service and the availability of related internet and phone tracking services, speed of delivery, and to reduce their risk of arrest during the transportation of drugs from one place to another. They often use hand-written airbills, drop the packages near closing time, pay for such services in cash and use false or nominee names, addresses, and/or telephone numbers when using such services in order to further insulate themselves from detection by law enforcement. Drug dealers frequently maintain records relating to their use

of these services, such as receipts, copies of airbills, empty and/or previously used boxes, packing tape, packing popcorn/filler and other packaging materials, and package tracking records printed from the internet, at their residences, stash houses, and/or in their vehicles where they are available for reference.

108. With respect to money launderers, I know money launderers can maintain large sums of cash in multiple locations that are within their control. This allows launderers to quickly disperse cash to their clients if the need arises. I know money launderers often establish businesses that are service businesses or "cash businesses" in order to more easily hide or otherwise obscure the true earnings of said businesses—which are typically much lower than reported to government entities, such as the Internal Revenue Service or state tax department. A business such as this allows launderers to place, conceal, and cycle ill-gotten cash proceeds through such a business with greater ease as compared to a business that is heavily regulated or predominantly works with traceable funds (such as wire transfers, cashier's checks, personal checks, and credit card transactions).

109. Businesses aside, I know money launderers also use other methods of laundering, such as the use of funnel bank accounts, wire transfers, or currency exchanges to conduct their money laundering activities. In the instance of using bank accounts or funnel bank accounts, launderers will work to keep their transaction amounts under the \$10,000 threshold that would

trigger a Cash Transaction Record with financial regulators. In this instance, money launderers will often use a number of people (or "smurfs" or "runners") to place these sub-\$10,000 increments into a bank account or accounts.

110. Based on my training and experience, and conversations with other law enforcement personal who have been trained specifically in cryptocurrency methods used by drug traffickers and money launderers, traffickers and money launderers will, at times, use cryptocurrency and cryptocurrency exchanges in an effort to thwart and evade law enforcement due to the encryption and anonymity many cryptocurrency services provide. Additionally, this currency can be moved very quickly, across the planet, which makes it even more attractive to money launderers.

111. Finally, I know that the commission of the SUBJECT OFFENSES in the manner set forth above necessarily requires the use of computers, smart phones, tablets, or other computer devices and storage media for the perpetrator to access dark web marketplaces and cryptocurrency exchanges and wallets, connect with customers, and co-conspirators, and engage in transfers of digital currency. I have learned through training and experience that individuals who engage in the SUBJECT OFFENSES in this way also commonly use such electronic devices to keep track of suppliers, customers and co-conspirators, keep records of illegal transactions and criminal proceeds, and store copies of online chats, emails, and other data. In addition, I know, based on training and experience that perpetrators maintain copies of

software programs and other applications to assist with accessing the dark web and running a vendor account, including, but not limited to, Tor browser software, cryptocurrency client and wallet files, digital signature software and related authentication keys, as well as encryption software and related encryption keys. In such cases, I know that perpetrators often keep such electronic devices inside their homes. In the case of smart phones, tablets, and laptop computers, perpetrators may also keep such devices on their person, either in their pockets or in containers such as carrying bags, cases, backpacks or protective sleeves.

112. Because RABULAN, GOLDBERG, and KUEKER's crimes involve the use of cryptocurrency and encryption, the items to be seized could be stored almost anywhere within SUBJECT PREMISES 1-3, in both physical and electronic formats. For example, Attachment B seeks cryptocurrency addresses, private keys, recovery seeds, PGP keys, and passwords. These pieces of data comprise long and complex character strings, and in my training and experience I know that many cryptocurrency users write down or otherwise record and store such items because they are too long to commit to memory. As such, these keys, passwords, and addresses may be documented in writing and secreted anywhere within a residence. For all of the foregoing reasons, your affiant respectfully submits that probable cause exists to believe that such records, data, and documents will be found within SUBJECT PREMISES 1-3, including in computers or on other devices that store electronic data.

**VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES<sup>8</sup>**

113. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

---

<sup>8</sup> As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

114. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

115. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a



device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

2. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress RABULAN's, GOLDBERG's, KUEKER's, MEIR's, and RAMIREZ's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of RABULAN's, GOLDBERG's, KUEKER's, MEIR's, and RAMIREZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

3. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

#### **IX. CONCLUSION**

116. For all of the reasons described above, there is probable cause to believe that RABULAN, GOLDBERG, and KUEKER have committed a violation 21 U.S.C. § 846. There is also

probable cause that the items to be seized described in Attachment B will be found in a search of SUBJECT PREMISES 1, 2, and 3 described in Attachments A-1, A-2, and A-3 of this affidavit and that the items described in Attachment B found in a search of RABULAN's and KUEKER's person as described in Attachments A-4 and A-5 of this affidavit.

117. Further, on the basis of the evidence described herein, I submit that there is probable cause to believe that any cash and cryptocurrency such as bitcoin constitute property involved in a violation of 18 U.S.C. § 1956 is traceable to such property. I further submit that there is probable cause to believe that the cash and cryptocurrency constitute property constituting, or derived from, proceeds obtained, directly or indirectly, as the above violations.

118. Here, because the above described property is mobile and can be easily moved, concealed, or transferred, a protective order under 21 U.S.C. § 853(e) may not be sufficient to ensure that the property remains available for forfeiture. Therefore, I request the Court to authorized seizure of the property under

///

///

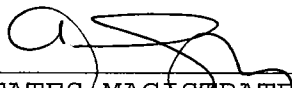
///

21 U.S.C. § 881(a)(6) (civil forfeiture) and 18 U.S.C.  
§ 982(a)(1) (criminal forfeiture).



Andrew Kim, Special Agent  
Homeland Security  
Investigations

Subscribed to and sworn before me  
this 18<sup>th</sup> day of March, 2019.



UNITED STATES MAGISTRATE JUDGE

**ALKA SAGAR**